ENHANCING ORGANIZATIONS’ ADAPTIVE CAPACITY AND RESILIENCE THROUGH EFFECTIVE DECISION-MAKING IN THE RECOVERY PHASE

Pages: 3-19 Authors: Dr Dean Myburgh, Chris Webb and Dr Erica Seville

Abstract: Complex, disruptive, events require sound leadership and an ability to effectively address uncertainty. Applying effective decision-making to meet the challenges created by emergencies and disasters requires leaders to consider and balance their thinking with that of others and to engage in new approaches to emergency decision-making.

This paper examines decision-making as an indicator of adaptive capacity and resilience in organizations within the recovery context. In particular, it draws on three frameworks for applying ‘whole-brained’ thinking as an organizing principle for decision-making in post-disaster (recovery) situations. It also highlights generic (but typical) decisions in simulated civil defence emergency management recovery contexts and offers insights into ‘whole-brained thinking’ constructs as developed by Herrmann (1994).

RESILIENT SOCIETIES: PERCEPTIONS OF THE IMPORTANCE OF BCM IN RESPONDING TO ENVIRONMENTAL RISK

Pages: 20-30 Authors: Paula Sonja Karlsson and Dawn Anderson

Abstract: Climate change is perceived to be one of the biggest threats to the future of an organization, yet, it has also been acknowledged there is an upside to such risk. An organization can gain a competitive advantage through the use of business continuity management (BCM) to help safeguard against future adverse incidents. This paper explores the relationship between the application of BCM within an organization and increased environmental risk. Specifically, it focuses on whether an increase in environmental incidents caused by climate change has seen an increase in the use of BCM by organizations to offset such threats.
Other papers

**DISASTER RECOVERY TESTING: IN A VENDOR RICH ENVIRONMENT**

**Pages:** 31-37  **Author:** Martin Welsh

**Abstract:** In the accelerating global economy, where companies turning to IT services providers is becoming much more commonplace, disaster recovery testing has become more complex. It can be argued that the need for a documented, comprehensive, actionable and accurate technology disaster recovery plan is more important now than ever before. This paper will discuss what pitfalls to avoid and how to update your disaster recovery plans so that you are testing the plan and not planning the test.

**IMPLEMENTING A BCMS AND GETTING CERTIFIED: AN ANALYSIS ACROSS GEOGRAPHIES**

**Pages:** 38-43  **Author:** Dhiraj Lal

**Abstract:** This paper focuses on similarities and differences in the effective implementation of business continuity management across diverse cultures, particularly in emerging/developing markets, such as the Middle East and Africa. The paper argues that any BCM implementer or consultant can increase his or her effectiveness by understanding the organization’s culture and the geography in which it operates and should accordingly tailor-make the BCM implementation approach, for maximum effectiveness.

**RESEARCH ROUNDPUP:**

**SUMMARIES OF RECENT COMMERCIAL AND ACADEMIC BUSINESS CONTINUITY AND RESILIENCY RESEARCH**

**Pages:** 44-51
ENHANCING ORGANIZATIONS’ ADAPTIVE CAPACITY AND RESILIENCE through effective decision-making in the recovery phase

By Dr Dean Myburgh, Chris Webb and Dr Erica Seville
ABSTRACT: Complex, disruptive, events require sound leadership and an ability to effectively address uncertainty. Applying effective decision-making to meet the challenges created by emergencies and disasters requires leaders to consider and balance their thinking with that of others and to engage in new approaches to emergency decision-making.

This paper examines decision-making as an indicator of adaptive capacity and resilience in organizations within the recovery context. In particular, it draws on three frameworks for applying ‘whole-brained’ thinking as an organizing principle for decision-making in post-disaster (recovery) situations. It also highlights generic (but typical) decisions in simulated civil defence emergency management recovery contexts and offers insights into ‘whole-brained thinking’ constructs as developed by Herrmann (1994).

Authors

**DR DEAN MYBURGH** is an industry researcher and member of the Resilient Organizations Research Team, an HBDI® Certified Practitioner and member of the Herrmann International global network, and also director of Confluence Group, 80-20 Options NZ Ltd and Emergency Planning Ltd.

**CHRIS WEBB** is head of the Auckland University of Technology (AUT) School of Paramedic and Emergency Management, an HBDI® Certified Practitioner and member of the Herrmann International global network.

**DR ERICA SEVILLE** is co-leader of the Resilient Organizations Research Programme, an adjunct senior fellow with the Department of Civil and Natural Resources Engineering at the University of Canterbury and also director of Risk Strategies Research and Consulting.
Introduction

Emergency and disaster events are becoming more prevalent and more complex in nature with serious implications for communities (Newkirk, 2001; United Nations, 2004, 2007; Cutter & Emrich, 2005; Rodriquez et al. 2007). The United Nations Human Settlements Programme’s global report (2007 p. 163) states: “As cities grow, disaster risk often increases through the rising complexity and interdependence of urban infrastructure and services, greater population density and concentration of resources. Yet, urban growth need not necessarily result in increased disaster risk.”

The complex interrelationships found in fast-growing urban environments demand new approaches for effective decision-making in disaster recovery situations. Flexibility, as well as both personal and organizational resilience, is required to recover the disrupted situation to a ‘new normal’. Effective decision-making is an implicit part of the leadership that is required in post-disaster situations.

Complex, disruptive, events require sound leadership and an ability to effectively address uncertainty. Applying effective decision-making to meet the challenges created by emergencies and disasters requires leaders to consider and balance their thinking with that of others and to engage in new approaches to emergency decision-making.

The role of effective decision making in improving resilience

Since knowledge about (and control over) the physical and social environments will always be evolving and inadequate, decision-making plays a key role integrating and aligning efforts to reverse the trend towards increased vulnerabilities. While it is not possible to eliminate all vulnerabilities, improving organizational resilience through effective decision-making will play its part in integrating safety, prevention and preparedness into the development of a more pro-active culture for disaster and emergency management. Enhanced decisions involve holistic processes where both vulnerabilities and resilience are considered.

This paper examines decision-making as an indicator of adaptive capacity and resilience in organizations within the recovery context. In particular, it draws on three frameworks for applying ‘whole-brained’ thinking as an organizing principle for decision-making in post-disaster (recovery) situations:

- McEntire (2001) offers a framework that is centred on the concept of vulnerability management. This framework also provides a useful basis for considering the decision-making approaches required to pro-actively address emergencies.
- McManus et al. (2007) provide another framework for decision-making that applies to building organizational resilience and post-disaster reconstruction. This framework and the supporting resilience measurement tool has been further refined in the more recent research completed by Stephenson et al. (2010).
The Herrmann Brain Dominance Instrument (1994) profiles the extent of whole brained thinking and offers a validated organizing principle that facilitates understanding of decision-makers’ thinking preferences both in normal circumstances and when under pressure. Bass and Riggio (2008) state that: “each year our understanding of transformational leadership grows in significant ways... yet leadership is perhaps the most complex of human constructs, and we still have a long way to go” (p. 263).

The paper highlights generic (but typical) decisions in simulated civil defence emergency management recovery contexts and offers insights into ‘whole-brained thinking’ constructs as developed by Herrmann (1994).

Effective decision-making in recovery situations

Effective decision-making is central to, and especially important in, the recovery process following disasters. The timeline for decision-making in the recovery phase tends to be longer and involves higher levels of complexity than for the response phase, where the focus is on swift actions to primarily save lives and then focus on securing critical infrastructure and assets. So what constitutes good decision-making in recovery?

Chandler (2008) emphasises the need for fast and effective decision-making in disaster recovery and the impact that crisis situations have on the capacity to make high quality decisions. A number of factors may diminish decision-making during critical events, including time constraints, emotional stress, fragmentary (and changing) information “facts” and external pressures. On the other hand, there are a number of key psychological and communication variables that can affect decision making during crises and emergency contexts.

Musselwhite (2009) surveyed 40,000 managers and identified five distinct decision-making preferences; of these five preferences, three (Investigating, Collaborating and Teaming) involve sharing with and engaging others. He states that ‘The practice of integrating knowledge of the five decision-making styles with consideration of each of the five key factors has been proven to enhance decision-making capability...(and) helping leaders ... learn how to adapt their decision-making style to produce the most effective outcome. Increasingly challenged to reduce the risk from poor decisions and increase positive results from good decisions, leaders must learn how to choose the best way to decide in any given situation’ (p.7).

According to Musselwhite, the appropriate degree of inclusion can be determined by considering the following five key factors (when each of these factors is fully considered, the style of decision making that will produce the best outcome becomes clearer):

- Problem clarity (consideration of the nature and scope of the problem);
- Information (facts and knowledge needed to make the best decision);
- Level of commitment (degree of buy-in and support needed to implement the decision);
- Goal agreement (degree to which stakeholders have common or competing goals among themselves and with the organization);
- Time (the degree of urgency surrounding the decision and the time and effort others must make to participate in the decision-making process).
Seville et al. (2009) concluded that responsive and resilient organizations generally practice participative management in which responsibility and decision-making is devolved to middle / lower organizational levels. Engaging others in the organization, including drawing on the different decision-making perspectives of those at different levels, helps ensure that the widest pool of talents and ideas is available to contribute to the task in both ‘business as usual’ and emergency circumstances.

Stephenson et al. (2010) identified leadership and decision-making as key indicators of the ‘adaptive capacity’ component of organizational resilience. Decision-making is seen as a key dimension in their Leadership, Management & Governance Structures indicator of resilience, which is defined as: ‘Organizational leadership which successfully balances the needs of internal and external stakeholders and business priorities, and which would be able to provide good management and decision-making during times of crisis.’ (p.36 - emphasis added). It also features in their Devolved & Responsive Decision-making resilience indicator which they define as: ‘An organizational structure, formal or informal, where people have the authority to make decisions directly linked to their work and where, when higher authority is required, this can be obtained quickly and without excessive bureaucracy,’ (p.37- emphasis added.)

Vulnerability management – a focus on managing both liabilities and capabilities

Understanding vulnerabilities and what these mean in the context of enhanced organizational resilience is an important consideration in the decision making processes associated with recovery management. McEntire (2001) offers a perspective regarding the vulnerability of organizations and how leadership manages these vulnerabilities. He acknowledges that preparedness and response remain vital aspects of emergency management, but outlines the need to address mitigation (reduction) and recovery from large events. The (over) emphasis within emergency management of physical issues and response operations (sometimes overlooking social / organizational variables) is highlighted.

Vulnerability management is promoted by McEntire as a concept that addresses a lack of capability in both the physical environment as well as the social / organizational environment and involves considering the building of capabilities in the wider organizational environment. This approach proposes that physical risks are assessed, but that susceptibility (the level of social/organizational liabilities) is also addressed. It challenges the singular focus on hazards and the notion that sustainability as a desired end-state may be achieved. Rather, it encourages thinking that is inclusive of preparedness and response; and includes managing hazards, focusing on sustainability, taking mitigation measures, planning for recovery, environmental protection and social justice issues. This requires that a holistic decision-making approach is utilized to address the assessments, interpret the results and take steps to plan for, mitigate, respond to and recover from hazards and consequential emergencies.

McEntire (2004) extends the thinking around vulnerability management by suggesting that it is closely related to a number of disciplines that contribute to emergency management, namely: geography, meteorology, engineering, anthropology, economics, sociology, psychology, epidemiology, environmental science, political science, public administration, law (legal liability),
journalism, emergency management and homeland security. Vulnerability management thus has the potential to unify the perspectives from multiple disciplines and provides a framework for decision-making from a multi-disciplinary perspective. The application of a whole-brained thinking and decision-making approach (refer to Whole-brained approaches to Emergency Management below) using information derived from these disciplines and the assessed resilience of organizations makes for a very powerful, integrated and inclusive approach to emergency management.

McEntire determines organizational capability as being a function of in-built resistance and resilience. While he focuses on the management of vulnerabilities, mitigation measures and building resilience, he does not fully address the concept of resilience. The concept of organizational resilience, as briefly mentioned in McEntire’s framework, is expanded upon later in the paper by McManus et al, (2007) who offer an alternative and complementary paradigm for decision-making in emergency situations.

It is also useful to consider the interaction of increased vulnerabilities in the following areas: physical, social, cultural, political, economic and technological. McEntire (2001) summarises the factors that augment vulnerability in table one. These factors provide guidance and a structure for decision-making that mitigates (reduces) and facilitates recovery. They also facilitate the creation of a more holistic view for managing vulnerabilities.

According to Wisner (1998) it has been observed that the capacity of individuals to cope with and recover from extreme events is reduced by several constraints. These include lack of access to information, financial credit or services and a lack of resources (e.g. assets and social support). The same may be said of decision-making in organizations that does not facilitate an inclusive holistic approach.

**Organizational resilience – building capacity and capability**

While resilience and vulnerability have implications for decision-making at a community level (e.g. the vulnerability and needs of groups at risk), they are equally relevant at an organizational decision-making level. It is imperative that leaders engage in effective decision-making for planning, creating capacity and capability, whilst reducing vulnerabilities and liabilities within their organizations in order to also play their part in the community context.

These decisions will play a wider community role, while also adding value to those organizations in the short-, medium- and longer term in terms of both reputation and the bottom line.
Table one: The factors that augment vulnerability and guide decision-making for managing vulnerabilities. (Source: McEntire, D.A. (2001): Triggering agents, vulnerabilities and disaster reduction: towards a holistic paradigm.)

McManus et al (2007) address the indicators of resilience in organizations and describe a resilient organization as one that not only survives, but is also able to thrive in an environment of change and uncertainty. Further, they state that resilience is the capacity to maintain and regain form and function. It requires conscious and responsive decision-making from leaders to make this happen.

The authors have expanded on the work completed by McManus et al. by including decision-making dimensions that are linked with the framework’s resilience indicators. The expanded matrix (refer to table two) offers decision-makers a holistic framework for addressing the building of capacity and capability within key areas in organizations. Decision-making considerations within each indicator of resilience are highlighted in order to assess resilience from a decision-making perspective.

Improved decision-making that involves engagement of key contributors throughout the organization (as well as key external contributors) requires embracing changed thinking about the devolution of responsibilities.
<table>
<thead>
<tr>
<th>INDICATORS OF RESILIENCE *</th>
<th>Situation Awareness*</th>
<th>Management of Keystone Vulnerabilities*</th>
<th>Adaptive Capacity*</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECISION-MAKING DIMENSIONS**</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Leadership, governance and decisions about resilience in people | • Communication, competencies and relationship management  
• Roles and responsibilities | • Competencies, learning and development | • Strategic Vision and outcome expectancy  
• Propensity for co-operation and supporting vs. a silo mentality |
| Decisions about resilience in processes | • Understanding of hazards and consequences | • Planning Strategies, participation in futures thinking and exercise scenarios | • Information and knowledge |
| Decisions about resilience in systems | • Systems aligned with strategic objectives  
• Connectivity and dependency awareness | • Organizational connectivity | • Information and knowledge |
| Decisions about resilience in information for decision-making | • Connectivity and dependency awareness | • Capacity and capability of internal resources | • Information available and supports decision-making |
| Decisions about resilience in revenue streams / financial arrangements | • Risk and Insurance awareness | • Capacity and capability of internal / external resources | • Alternative / flexible revenue arrangements |
| Decisions about resilience in assets | • Holistic view of assets and their role in business success  
• Maintenance and recovery priorities | • Capacity and capability of internal resources | • Assets well maintained, with in-built redundancy |
| Decisions about resilience in infrastructure | • Holistic view of the role of infrastructure in business success  
• Maintenance and recovery priorities | • Capacity and capability of internal resources | • Infrastructure that can support business-as-usual and extreme requirements |
| Decisions about resilience in other organizational dimensions | • Integration of all dimensions into a holistic organizational resilience framework | • Organizational connectivity | • Ability to link with, support and enable other organizational dimensions |

Table two: The Organization Resilience Matrix – a decision-making framework for assessing resilience in organizations.
In order to build capacity and capability in organizations (building resilience), decision-makers need to address all of these indicators and dimensions in both business-as-usual and emergency situations. The authors propose that decision-makers use a combination of McEntire’s vulnerability management concept and the Organization Resilience Matrix to reduce liabilities and consider the building of capacity and capability in organizations; the use of the Organization Resilience Matrix is suggested as part of an integrated approach to building resilience in key areas. This facilitates thinking about key considerations related to reducing vulnerabilities, enhancing organizational resilience and ensuring that decisions related to recovery ensure better outcomes.

**Whole-brained approaches to emergency management**

Herrmann International’s Whole Brain methodology (1994) is based on proven research into how people think and communicate. Thinking preferences have an impact on virtually everything we do, including communication, decision-making, problem solving and management styles.

The Herrmann Brain Dominance Instrument (HBDI®) underpins Herrmann’s Whole Brain methodology. The HBDI® is a well-known and validated instrument that has been used for over 25 years to evaluate and depict the thinking preferences and styles of individuals and members of teams in each of the four brain quadrants - upper left and right; lower left and right. By understanding and harnessing the thinking styles and preferences of individuals, teams and organizations are in a better position to enhance decision-making that combines analytical, organizational, strategic and interpersonal skills (Herrmann, 1994). The authors propose that this instrument (and its profiles that indicate thinking preferences under pressure) has application in decision-making in organizations that wish to reduce vulnerability, enhance resilience and adaptive capacity which, in turn, assists the recovery of organizations following crises.

Different thinking and responses are required in emergency recovery situations and decision-makers need to allocate tasks on the basis of a clear understanding of individual team members’ thinking and how they react under pressure. Armed with these insights, the decision-maker is in a stronger position to assess task allocation, the dependency of individuals and teams, and inter-personal dynamics that support or detract from the desired outputs and outcomes.

**Research methodology**

During the period 2008 to 2010, a group of managers engaged in studies about leading and making decisions in emergency situations were profiled using the HBDI® to ascertain the effectiveness of this approach. All of these managers were engaged in emergency management studies at Auckland University of Technology (AUT) and held leadership roles with decision-making responsibility in emergency service agencies. Profiles were plotted using information derived from a series of 120 questions that measure the degree of preference between each of the four individual thinking structures (quadrants) and the extent of left-brain, right-brain, cerebral and limbic thinking (referred to as thinking modes). This resulted in a four quadrant profile for each participant that displayed the degree of thinking preference for each of the four quadrants. These individual profiles were then plotted onto an HBDI® Quadrant Chart (shown in figure one) to gain an understanding of the
differences in their individual thinking and decision-making preferences. HBDI® scoring results are free of value judgement and cultural bias.

Figure one: Plot of HBDI® profiles of survey participants (emergency management practitioners.)

Participants were then tasked with completing a Recovery Management Survey that required them to individually prioritise decisions, based on a recovery scenario. Participants in this study were asked to consider 23 selected recovery decisions (typical recovery tasks) and consider the thinking / decision-making aspects related to each task; they were asked to consider and prioritise the top eight decisions in the recovery scenario that they were given. They were also asked to include a brief statement explaining the rationale for each decision.

The research then allocated these top eight decision selections according to the HBDI® quadrants as follows:

- Top-left quadrant (focusing on facts)
- Bottom-left quadrant (focusing on form – planning and implementation)
- Top-right quadrant (focusing on future)
- Bottom-right quadrant (focusing on feelings or people considerations.)

Table three shows the whole-brained thinking reflected in the 23 recovery decisions across the four HBDI® quadrants. The authors drafted the statements relating to these recovery decisions to introduce the full spectrum of thinking that may apply to a recovery scenario (on the one hand) and an element of prioritisation (or forced-choice) between different decision-making elements.
Table three: Whole-brained thinking and decision-making in recovery.

Effective (whole-brained) decision-making for recovery involves thinking from all of the quadrants. Unless a leader as decision-maker is confident that the emergency management recovery team is whole-brained in its approach (using the thinking from all of the quadrants in decision-making) and is able to address all of these dimensions, the results are likely to be sub-optimal and not provide sufficient focus to the desired recovery outputs and outcomes. Equally important is how the leader approaches the decision-making process while under pressure. Each of the quadrants is discussed with examples of how this relates to decision-making.

<table>
<thead>
<tr>
<th>FOCUS ON FACTS</th>
<th>FOCUS ON FUTURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Effectiveness of the volunteer programme is evaluated.</td>
<td>• Consideration of appropriate supplier and other support arrangements for recovery.</td>
</tr>
<tr>
<td>• Independent review and evaluation of recovery plan / exercises.</td>
<td>• Following the recovery process, future recovery strategies are developed.</td>
</tr>
<tr>
<td>• Financial systems and budgets for recovery have been considered.</td>
<td>• Reduction measures are considered for incorporation into district and regional plans for future recovery planning.</td>
</tr>
<tr>
<td></td>
<td>• Considering appropriate messages for delivery to the public about recovery processes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FOCUS ON FORM</th>
<th>FOCUS ON FEELINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Distinguishing between my normal business role and my allocated recovery role.</td>
<td>• Engaging all recovery team members in regular recovery training and exercises.</td>
</tr>
<tr>
<td>• Clarifying roles and responsibilities for recovery.</td>
<td>• Articulating and communicating recovery plans and procedures to recovery team members.</td>
</tr>
<tr>
<td>• Volunteers have a work programme / plan to work to.</td>
<td>• The community are engaged and know where to go to in a disaster e.g. welfare centres.</td>
</tr>
<tr>
<td>• Prioritisation process for allocation of resources in recovery.</td>
<td>• Development of appropriate relationships between and with agencies and organizations involved in recovery.</td>
</tr>
<tr>
<td>• Key contacts in agencies involved in recovery have been identified.</td>
<td>• Development of appropriate relationships with the media.</td>
</tr>
<tr>
<td>• Conducting impact assessments and analysing the results during recovery.</td>
<td></td>
</tr>
<tr>
<td>• Documentation of recovery Standard Operating Procedures (SOPs), e.g. Operation of Emergency Recovery Office.</td>
<td></td>
</tr>
<tr>
<td>• Identification and equipping of recovery facilities in the community e.g. welfare centres.</td>
<td></td>
</tr>
<tr>
<td>• Plans for temporary accommodation during the recovery phase.</td>
<td></td>
</tr>
<tr>
<td>• Development of systems to enable inter-agency co-operation, assessment of needs and management during recovery.</td>
<td></td>
</tr>
<tr>
<td>• Establishment and maintenance of an up-to-date database of all welfare-related agencies.</td>
<td></td>
</tr>
</tbody>
</table>
The decision choices selected and prioritised from those shown in Table three and the supporting rationale were analysed in terms of thinking preferences. The extent of whole-brained thinking (and application of the HBDI® thinking preference concepts and language to each action) was then evaluated in order to assess whether their awareness and learning about whole-brained thinking made for more balanced decision-making in the given recovery scenario. Multiple responses or ‘loadings’ within any given quadrant were noted, together with recovery decisions that have a ‘left-brained’ (blue-green) or ‘right-brained’ (yellow-red) orientation.

Discussion and interpretation of the results

The decision choices presented to respondents that related to the recovery scenario were analysed to gauge the degree of balance in the decisions/approaches taken.

Overall, of all responses/decisions choices made by all respondents (refer to Figure two) there was a low preference for focusing on facts; although only three out of the 23 recovery decision choices available related to ‘a focus on facts’, only five percent of the 96 actual decision choices made related to using facts and data (information); this relates to evaluation, data collection, financial and technology considerations and how performance is to be measured in the recovery process. This under-representation in actual decision choices points to the potential for such important considerations to be excluded from the consideration of recovery priorities.

![Graph: Actual recovery decision choices compared with available recovery decision choices (by HBDI Quadrant)](image)

Figure two: Results for all survey respondents.

Responses across other quadrants indicated a balance in decision-making related to:

- Using planning processes, deciding on the timing of implementation, administrative processes and quality of outcomes/outputs (Bottom-left quadrant that focuses on form – planning and implementation); 41 percent of top eight responses reflected that this type of decision-making would receive priority;
- Using consultation, partnerships and other communication and people considerations in its implementation; 32 percent of top eight responses reflected that this type of decision-making would receive priority;
- Using strategy, a clear vision and consideration of desired future states; 22 percent of top eight responses reflected that this type of decision-making would receive priority.
Notably, decision choices that were fact-based or analytical were significantly under-represented across all responses (5 percent) compared with the 13 percent of fact-based or analytical decision choices that were available.

The key learning from the above is that facts and supporting data may not receive sufficient attention in the recovery decision-making process.

Herrmann’s Whole Brain methodology (1994) describes analytical decisions (facts) and procedural / process decisions (form) as left-brain thinking; ‘big-picture’ decisions (about the future) and decisions involving consideration for people and communication (feelings) represent right-brain thinking.

A summary of the percentage of actual left- and right-brain responses compared with available decision-choices (i.e. the proportion that the left- and right-brain quadrants is represented in the total number of available decisions for inclusion in the top eight) is shown in figure three. The actual recovery decisions of all respondents that focused on Future and Feelings (people) were proportionally higher (54 percent) than the 39 percent of available decision choices.

![Figure three: Left- and Right-brained recovery decision choices.](image)

Actual recovery decisions that focused on Facts and Form were proportionally lower (46 percent) than the 61 percent of available decision choices. This may be reflective of the factors that diminish decision-making during critical events (Chandler, 2008).

The key learning from the above is that facts (and supporting data) as well as form (process and procedure) may not be given sufficient priority in recovery decision-making.

**Rationale for most frequently selected recovery decisions**

Table five summarises the rationale provided by respondents for the most frequently selected recovery decisions. This summary of the rationale for recovery decisions clearly indicates an under-utilisation of facts (and data / information based on evaluation, data collection, financial and
technology considerations (and how performance is to be measured)) in the recovery decision-making process.

<table>
<thead>
<tr>
<th>Recovery decision</th>
<th>Rationale</th>
</tr>
</thead>
</table>
| Considering appropriate messages for delivery to the public about recovery processes | • Giving the right messages  
• Avoiding confusion and creating unrealistic expectations  
• Empowering public to make decisions that enhance their own recovery  
• Creating confidence in the recovery process  
• The development of key messages (about the future)  |
| Clarifying roles and responsibilities for recovery | • Perception reinforced that something is being done to facilitate the recovery (by doing)  
• Summary of the individual and collective skills that team members can bring to the recovery team / recovery process  
• Knowing respective roles and responsibilities during the recovery operation  
• Enabling performance & reducing stress around role ambiguity  
• Training and input in to recovery plans / procedures  |
| Development of appropriate relationships between and with agencies and organizations involved in recovery | • Clear communication and understanding between agencies  
• Forging relationships with key organizations /stakeholders before and during the recovery phase to ensure recovery objectives are achieved  
• Relationships established with the key players  
• Engagement of the recovery team  |
| The community are engaged and know where to go to in a disaster e.g. welfare centres | • Involvement in the development and consultation of recovery plans and procedures  
• Participation in recovery exercises and related learning  |

**Key:**

**Future:** how decision-making is applied to recovery, using strategy, a clear vision and consideration of desired future states.

**Form:** how decision-making is applied to recovery, using planning processes, deciding on the timing of implementation, administrative processes and quality of outcomes / outputs.

**Feelings:** how decision-making is applied to recovery, using consultation, partnerships and other communication and people considerations in its implementation.

*Table five: Rationale for most frequently selected recovery decisions.*
Thinking under pressure

Under-pressure profiles of respondents indicate how their thinking changes and how they respond when under pressure. For respondents with a focus on Future and Feelings, their pressure profiles confirmed a low preference or avoidance of fact-based or analytical decision-making. An analysis of the under-pressure profiles of respondents indicated that 50 percent of all respondents have a low preference (or avoidance) of fact-based or analytical decision-making. This may have contributed to and partly explain the low number of decision choices involving fact-based decisions.

This offers the opportunity to consider the influence that thinking preferences have on key emergency management decision-making choices, especially during the post-disaster (recovery) phase. In relative terms, decision-making during recovery is challenged by complexity rather than the speed with which decisions are made. Reflection that facilitates holistic decision-making to address the complexities and varying nature of recovery situations is vital if organizations are to enhance effective, responsive and devolved decision-making.

The survey results indicate the potential for exclusion of important considerations from decision-making related to recovery priorities. Whether making decisions as individuals or in teams, an awareness of tendencies to avoid fact-based or analytical decision-making would facilitate more balanced and whole-brained (holistic) recovery decisions.

Longer timelines for decision-making in recovery allow for recovery decision-making involving team members; an awareness of the team’s decision-making preferences will provide a basis for determining the extent to which ‘balanced’ or whole-brain thinking has been applied in recovery decision-making.

Conclusion

All three frameworks that have been explored in this paper emphasise a holistic approach to decision-making. The vulnerability management approach discussed by McEntire (2004) offers a framework for decision-making from a multi-disciplinary perspective framework; this ‘multi-disciplinary thinking’ implicitly supports the thinking preferences approach as outlined by Herrmann (1994). The frameworks for decision-making that apply to building organizational resilience and post-disaster reconstruction as outlined by McManus et al. (2007) and Stephenson et al. (2010) provide a further basis for enhancing decision-making when under pressure. Decision-making that forms part of the recovery process may be enhanced by considering key variables within the ‘vulnerability management’ and ‘organization resilience’ frameworks.

In context of these frameworks and approaches to enhancing organizations’ adaptive capacity and resilience, an understanding of team members’ HBDI® profiles and the degree of ‘slant’ in their decision-making adds another dimension to effective recovery decision-making. As highlighted in the survey findings in this paper, facts (and supporting data) as well as form (process and procedure) may not be given sufficient priority in recovery decision-making. Awareness and understanding of a recovery team’s avoidance of fact-based decisions promotes a more balanced approach to decision-making (i.e. whole-brain thinking), making for better recovery outcomes. The whole-brained thinking
organizing principle offers those dealing with emergency situations an alternative decision-making approach (whole-brained decision-making in emergency management) that encompasses all of the aspects (facts, form, feelings and future) that demand consideration.

The opportunity for further enhancement of disaster and recovery management decision-making using whole-brained approaches (with HBDI® profiling) has been illustrated by sharing the research results obtained from the prioritisation applied by a group of experienced emergency managers to a set of decision-making choices within a recovery scenario that they were presented with. By using the approaches described, those involved in emergency situations are better-equipped to demonstrate pro-active decision-making in their approaches to managing recovery and other emergency management processes.

Whole-brained approaches (using HBDI® profiling) offer decision-makers the opportunity to review and evaluate both the nature of decisions (i.e. which decision quadrants they are addressing) and the extent to which they contribute to a balanced consideration of all important recovery components.

References


RESILIENT SOCIETIES:
Perceptions of the importance of BCM in responding to environmental risk

By Paula Sonja Karlsson and Dawn Anderson
**ABSTRACT:** Climate change is perceived to be one of the biggest threats to the future of an organization, yet, it has also been acknowledged there is an upside to such risk. An organization can gain a competitive advantage through the use of business continuity management (BCM) to help safeguard against future adverse incidents. This paper explores the relationship between the application of BCM within an organization and increased environmental risk. Specifically, it focuses on whether an increase in environmental incidents caused by climate change has seen an increase in the use of BCM by organizations to offset such threats.

Authors

**PAULA SONJA KARLSSON**
The first author, Paula Sonja Karlsson, holds a BA (Hons) and MSc in Risk Management, and is currently undertaking a PhD in Risk in the Department of Law, Economics, Accountancy and Risk at Glasgow Caledonian University. Her research interests are within fields related to societal risk, including community resilience, environmental risk and public sector risk. The research this paper is based on was conducted in fulfilment of her BA (Hons) degree under the supervision of Dawn Anderson.

**DAWN ANDERSON**
Dawn Anderson is a lecturer in the Department of Law, Economics, Accountancy and Risk at Glasgow Caledonian University. She has lectured on the undergraduate and postgraduate Risk Management degrees at the University for almost 10 years focussing predominantly on the fields of business continuity, crisis management, societal risk and insurance.

Acknowledgments

Thanks go to Claire McCann for her valuable contributions in the preparation of this paper. All research participants are also thanked for their input.
Overview

In recent years, a number of large environmental events have occurred with significant impacts on businesses and societies as a whole. For example, the “big freeze” that hit the UK in early 2010, caused substantial chaos, with economic and human costs, as well as causing difficulties in transport and energy consumption. Hurricane Sandy, which hit the US in October 2012, is the most contemporary reminder of the catastrophic impact that nature can have on societies.

Evidence suggests that the global climate will change significantly by the end of the 21st century, with potential impacts felt in economies, societies, natural environment and business. It is too complicated to predict the exact impact of climate change and which industries will be mostly affected [1, 2]. This supports the view that all organizations should engage in business continuity given this uncertainty.

Organizations are now much more subject to global risks of which environmental risk is one. In this paper, this is examined in terms of the increased risk this creates for interlinked organizations, whether generated by climate change related risks such as flooding or other weather related disruptions occurring regardless of climate change. Due to BCM being a relatively new discipline [3] and the concept of climate change still being debated [4], relevant literature linking climate change with BCM was limited, therefore the study aimed to address this gap. The aim of the study was to investigate the use of BCM in managing disruptions occurring as a result of environmental risks, focussing specifically on perceptions of the risk of climate change.

Methodology

Key literature was reviewed on the issues involved. In addition to this, perceptions of BCM and/or risk management experts were sought. The first author attended the Resilient Scotland Conference in November 2010 to gain the views of experts and practitioners in Scotland. In addition to this, four semi-structured interviews were conducted between January and February 2011. Interview participants were selected from the same geographical area, allowing for comparisons being made with organizations having experienced similar weather phenomena. The sample consisted of participants from the following sectors: local authority, financial services, aviation and engineering. While the overall issue is global, the sample that was used was UK based. The sample is however not representative of the whole population.

The engineering sector was chosen, as it may not have been under similar public scrutiny as some of the other sectors relating to recent environmental incidents. For the study this was perceived to be an important area to explore to see whether any changes had occurred. It was anticipated that a company in the aviation sector would have thorough hands-on experience of environmental risks due to the likelihood that it would already have experience of dealing with previous weather related incidents. A council was chosen, as contingency planning legislation such as the Civil Contingencies Act 2004 affects many public sector organizations and the authors wanted to gain a perspective
from this angle. Finally, it was of interest to explore how a global player such as a large UK bank needs to consider business continuity in relation to environmental risks.

Discussion of key literature

**Business continuity management and risk management**

BCM may not prevent incidents, but may help in mitigating the effects if an early warning is provided. In the case of environmental instability, BCM can support organizations to prepare for eventualities. It has been debated for some time now where business continuity should sit as a function within organizations. There are three views on this: business continuity is closely linked to risk management and should therefore sit side by side with it; business continuity is linked to risk management and should be an element of the risk management function; and business continuity is linked to risk management, but the order of hierarchy is not agreed upon [5].

The risk management function has long been established within organizations, counter to that of the business continuity function. The risk management function is by now relatively well understood and embedded in businesses and increasingly gaining importance [5, 6], whereas BCM is yet in its infancy in many organizations. BCM is related to IT recovery; due to organizations’ increased dependency of IT. Many organizations fail to treat BCM holistically covering all strategic processes, thus business continuity is not yet seen as a corporate issue that requires involvement of the board [7]. BCM should not be in contradiction to the overall goals and strategies of a business, but instead support the achievement of these by all means.

Whether BCM is viewed as a discipline on its own or as part of risk management in organizations should not be the main issue. The key point is how the profile of the function comes across: it must be communicated as something important for the organization’s success. Therefore the positioning of BCM is not totally irrelevant in so much as it should not be seen as inferior to the risk management function [8]. BCM should be used as part of normal business management processes as it adds value to organizations, resulting in cost efficiencies and improved product and service availability if a potential business disruption occurs [9].

**Opportunities**

Organizations are today recognizing the upsides of risk. It is increasingly acknowledged that organizations that have strong risk management processes in place will, with the associated enhanced resiliency, gain benefits such as greater competitive advantage, which will help the strategic growth of the business. This is where BCM will prove beneficial in the next few years, bearing in mind the increasing global changes. Although the challenges may be greater in today’s business environment, so are the opportunities [6].

According to a McKinsey Quarterly survey [10], climate change is perceived by executives to be an important issue, both in terms of risks and opportunities. Larger organizations are nowadays much more under public scrutiny in their dealings related to climate change, including sustainability and carbon footprint issues. The damage that inaction can have on reputation and profits should be a huge motivation for these businesses to take action. Smaller firms tend to be under less public
scrutiny which also may create problems. If no real pressure exists from the public, smaller companies may face the risk of not realising how big of a threat climate change actually is to the businesses future. Furthermore, if they are unaware of the threats, they most likely will be unaware of the opportunities posed in taking a proactive stance on climate change [11].

Resilience

The Civil Contingencies Act 2004 aims to generate a more resilient UK. As part of this aim it requires local authorities to aid and advise businesses and voluntary organizations about BCM matters [12]. However, it has also been suggested that businesses should assist the enhancement of community resilience, rather than leaving this up to the local authorities [13]. This is because no business operates in a vacuum, but, instead, companies have dependencies on the surrounding communities.

BCM is generally incorporated in large organizations, where huge losses can be expected and more resources to combat these are at hand [14]. It was noted by the experts at the Resilient Scotland Conference [15] that small and medium sized enterprises (SME) would not incorporate BCM until an event occurs that directly impacts on them, due to the costs involved with BCM. Nonetheless, smaller organizations should find it to be just as important to have BCM in place [16], due to the potential for suffering large losses from sometimes relatively small disruptions [14] as they have a smaller amount of resilience against disruptions compared to large organizations. In smaller firms business continuity could be kept fairly simple compared to the more complex plans in large organizations [3].

SMEs are a significant part of the UK economy, with Prime Minister David Cameron having stated that the future of Britain lies in small businesses, where a lot of growth potential exists [17]. For that reason, they should be supported by all appropriate means. This could be where larger organizations fit in in terms of aiding community resilience. Actions could include having a sharing scheme for recovery facilities. According to the experts at the Resilient Scotland Conference [15], it is important to de-mystify BCM, in the similar way that this was important for risk management. It must be made more simple and understandable so that SMEs can also get on board with it. SMEs must also be made aware of all the support that there is available for them in relation to BCM. This situation is changing, however, with the increased awareness of BCM [16].

Organizations are today realising the importance and the benefits that can be gained from sound risk management and business continuity [6]. This creates business resiliency, which is the next step in BCM [18]. Furthermore, it is of great importance that resilience should be built into processes from the very beginning [19]. It has been argued that the global challenges involved with climate change, are far more difficult and long-term to deal with than what BCM in its traditional sense was intended for, therefore it is of paramount importance for BC managers to strive for organizational resilience [20].

Contemporary organizations operate in a way that has created greater potential for, and increased the likelihood of, a variety of disruptions. Organizations are today much more vulnerable to outside events due to their dependency on various other businesses [21]. The increased importance of supply chain risk has raised the profile of BCM and many companies view disruptions in the supply chain as a significant risk to accumulating profits [22]. It has been further argued that globalisation is the largest opportunity and obstacle for organizations today [23]. Therefore, a lot of attention has
been put on the resiliency of supply chains and the importance of evaluating supply chains for an organization’s own continuity [24].

Business disruptions can happen anywhere in the supply chain [25]. The likelihood is that the incident happens externally and, as it is not directly its problem, the organization will rely on others to deal with it. Due to the interdependencies amongst businesses today, incidents will however, impact all sectors at the same time [26]. The problem with extensive use of supply chains is that the organization will lose some of its risk awareness and the visibility of risks [22]. Western organizations typically use suppliers from emerging markets, which is a necessity in today’s business environment due to the associated low costs, effectiveness and improved performance. Even small businesses depend on some form of outsourcing [25]. Yet in emerging markets, risk management practices are often non-existent or in their infancy, which could be disastrous for organizations along the supply chain [6].

**Barriers to implementation**

Some principal issues exist regarding business continuity today, one being the allocation of funding, where problems are exacerbated in times of recession [27, 28]. For example, terrorism is perceived to be a very high risk, which has, at least in the US, overshadowed the need to fund preparation for other hazards, including flooding and hurricanes, which are more likely [29]. Moreover, perceptions about disasters are mostly wrong; people still believe that disasters will not happen to them. Due to a false understanding about cost and probability, implementation of BCM cannot always be justified [14]. In reality, there are huge costs, both economically and psychologically, to organizations, the society and individuals who are affected by a crisis [21]. These costs are emphasized if no BCM is in place and even a small incident can be disastrous if the key dependencies are affected [14]. Therefore, in harsh economic times BCM should be maintained, rather than targeted as an area for cost saving [28].

It seems to be acknowledged now by scientists that climate change is upon us, albeit the cause of it is mostly under debate. Business continuity managers should see past the debates over the causes and should act proactively regarding climate change [4]. The impact of incidents such as Hurricane Katrina and Hurricane Sandy clearly show the influence that storms can have on both lives and property. More such storms can be expected, which will have enormous consequences. The important issue to realize about climate change is the possibility to adapt to the changing situation [30]. However, even though several organization’s find climate change to be a larger threat to their long term success when compared with terrorism and pandemics for instance, it seems that many organizations simply do not know how they should prepare for this prospect [31].

**Research findings and discussion**

**Importance of BCM**

With the exception of the engineering company studied, all organizations had BCM in place at the time of interviewing. The engineering organization representative explained that it was under development and that it will have a sharing scheme with its nearby offices, thus saving on direct financial costs. These sharing schemes could be extended outside the organization, which would
enhance the community resilience as well as saving costs. The potential for this was demonstrated by the council which was studied. The council had a recovery infrastructure that was shared with two other councils.

Whereas the aviation organization was fully on-board with BCM, stating that it is now part of the organizational culture, there were various levels of buy-in at the other organizations studied. It was pointed out by the representatives for the engineering company and the financial services institution that it is usual that the importance of BCM rises when things go wrong, whereby the importance of BCM is acknowledged, but if nothing has happened for a while it may be seen simply as an unnecessary cost. However, it was further noted by the representative for the financial services institution that with so many incidents having happened in recent years, it is easier to keep people’s focus on BCM nowadays. The council representative suggested that although they have the Civil Contingencies Act to guide them, there are still weaknesses in BCM, the ultimate difficulty being the amount of resources available. Business continuity cannot be a focus in the current climate due to lack of resources, said the representative. This was a view which was strongly opposed in the literature findings.

**Perception of environmental risk**

The representative for the financial services institution said that there are things that happen every year, but that severe weather was one that has become an issue to watch out for. Weather was a recurring theme throughout the interviews. The engineering services representative said they need to thoroughly prepare for weather related incidents, as, whatever happens, the company still needs to be able to deliver its products or services. There is strong evidence [1, 32 & 33] to suggest that companies should take account of climate change when doing their BCM plans.

Adverse weather and sustainability are issues that organizations must take very seriously. However, the engineering organization representative pointed out that this does not mean that other factors are any less important. The representative for the financial services institution agreed with this.

According to the representative of the aviation organization, the airport is becoming smarter in the way it deals with things, compared to how it used to be. In the past it was sufficient to tick a box where business continuity was concerned; but this was no longer the case. Environmental risk has now been escalated up to a key strategic priority.

The council representative explained that for the council the environment has always been looked at in terms of BCM due to the requirements set down in the Civil Contingencies Act; however, environment always comes after considering people and places first. Flooding is seen as the major issue in the council, but the increase in environmental risks has not changed anything in their procedures, as it already has been covered; particularly now with the multi-agency way of working. The latter means that the council has a greater awareness level and knowledge base.

**BCM as a tool**

According to the representative for the financial services institution, BCM is a vital tool for organizations, as without the thought of “what if” in case of an incident, organizations will end up not being resilient enough to keep critical functions going.
The engineering organization representative commented that rarely will the incident planned for occur, but something unplanned for often happens instead.

It was concluded by the representative for the financial services institution that incidents are always going to happen, especially when you are least expecting them. Risks such as flooding and severe weather can be anticipated and planned for, based on the vulnerabilities of every company [32], which was verified as having made the financial services institution focus more on the way they operate and how they could do things differently; for instance the increased ability for remote connectivity.

It was further argued by the representative for the aviation organization that the value of BCM increases immensely when something goes wrong, and that is when there is a huge focus on BCM.

The council representative noted that BCM is a form of security blanket, which helps to drive many decisions in the council. It helps the council to identify where they have weaknesses, and also has made it more resilient to both internal and external major incidents.

**Community resilience**

The representative of the financial services institution evaluates BCM in financial services to be relatively well embedded, but acknowledges that things can always be improved by looking at best practice from other organizations. He further estimated that councils and emergency services are quite good at BCM, but overall from his experience from other industries, the use of BCM seems to be quite mixed, and the smaller the organization, the less focus there will be on BCM due to lack of resources. This view was supported by the experts at the Resilient Scotland Conference [15].

The council representative argued that BCM should be something done by all organizations, even small corner shops, albeit maybe not to the same extent as it is done in larger firms.

As previously pointed out, SMEs are seen as vital to the UK’s economy and should be supported by all appropriate means. Therefore, the experts at the Resilient Scotland Conference [15] concluded that BCM must be de-mystified.

According to the council representative, there has been an increase in recent years in companies approaching the council to get information on BCM, but he disputed whether that has been due to any recent incidents, but rather suggested that it would be due to the council pushing more information out, as a result of the Civil Contingencies Act expecting councils to interact with communities. It was found in the literature that the increased awareness of BCM is due to the amount of information that is now available on the subject. The council representative however, believed that companies do not actually make a link between BCM and any adverse events, instead they just try to get through periods of disruption in an unplanned way.

According to the council representative, bad things need to happen, for businesses to see that they need BCM which was also the view of the experts at the Resilient Scotland Conference [15]. For instance, it is the councils that have endured incidents that have the best emergency plans in place now. The council representative concluded by saying that it is the small companies they need to target, and these are the hardest ones to convince. It was suggested in the literature that private organizations as well as local authorities should try to help SMEs with business continuity planning,
in order to enhance community resilience. This, in turn, helps protect the larger organization against supply chain risks. However, the representative of the aviation organization recognised that whilst trying to be proactive, even with the best intentions, one can never prevent all disasters and crises.

Recommendations

It was established that organizations now see environmental risk as a concern. This was demonstrated by the interviews, experts at the Resilient Scotland Conference and the literature. It has become apparent that people should be looking at adaptation strategies rather than focusing on the cause of climate change. It was, however, revealed that organizations do not know what exactly they should be doing. Clear guidance from the government and/or experts in the field should be given that is practical to implement.

The upside to risks has been identified, particularly in the context of gaining competitive advantage from successfully dealing with the key issues involved, such as supply chain and ‘green’ strategies. However, the opportunities posed by being prepared for climate change or being more environmentally friendly by operating in a sustainable manner, seem to be something organizations still fail to grasp, particularly SMEs. In the current economic environment where money is sparse it is anticipated that BCM is not on top of the agenda in many organizations. However, by investing in BCM, the opportunities may bring financial gains and/or savings to organizations that may in fact help alleviate the pressure of the economic situation.

The global challenges of climate change are much more complex to deal with than what BCM in its traditional sense was intended for and, as a result, many business continuity managers are broadening their horizons and are striving for organizational resilience. Organizational resilience, however, cannot be achieved unless there is community resilience. Today all organizations function in a much wider economy and market and this should be recognised in any decision making. If this factor is ignored it can have enormous consequences. Organizations must be aware and understand their dependency on external sources. Therefore, BCM in relation to climate change should, in the first instance, be about making communities more resilient.

In essence, all interviewees perceived BCM as a vital tool for organizational survival, but it was recognised that its use is still limited or non-existent in many organizations, particularly SMEs. It seems to be of key importance to de-mystify BCM in the same way as risk management had to be de-mystified, so that smaller organizations also understand its importance and see the value for their organization of implementing it.

Conclusions

The aim of the study was to investigate how different industry sectors in the UK use BCM to manage disruptions occurring as a result of environmental risks, focussing specifically on the perceptions of the risk of climate change. The focus on BCM has increased with recent events and its importance has been highlighted. If an event is dealt with successfully, it further promotes BCM, and can be used as a learning opportunity. It seems that in those businesses where BCM is already in place the function has got further positive recognition due to recent high-profile disruptions.
However, in order to create the resilient community proposed by the Civil Contingencies Act, organizations should work together in a proactive manner. It is the small firms that need to be targeted. They are the ones that need to be convinced of the effectiveness of BCM.

Ultimately, not all incidents can be planned for; but that is not to say that one should not try. The solution seems to be that certain outcomes, which can be devastating for critical activities, should be planned for. Climate change is something that is here to stay and should therefore be seen as a key risk, as it will change a number of key aspects for many businesses. Those that take action now, in order to adapt, will be better positioned when the changes are too large to ignore.

References


DISASTER RECOVERY TESTING:
in a vendor rich environment

By Martin Welsh
**ABSTRACT:** In the accelerating global economy, where companies turning to IT services providers is becoming much more commonplace, disaster recovery testing has become more complex. It can be argued that the need for a documented, comprehensive, actionable and accurate technology disaster recovery plan is more important now than ever before. This paper will discuss what pitfalls to avoid and how to update your disaster recovery plans so that you are testing the plan and not planning the test.

**Author**

**MARTIN WELSH**
Martin Welsh, CBCP, MBCI, leads the Disaster Recovery and Business Continuity practice within the IT Infrastructure Services business unit at Cognizant, a global provider of IT, consulting, and BPO services. As the Practice Lead, he is responsible for the development and support of DR/BC methodology, products and service delivery. As a DR/BC expert, he has product management, business development and hands-on experience developing IT and business recovery programs, strategies and services for Fortune 500 clients.
**Introduction**

In the accelerating global economy, where companies turning to IT services providers is becoming much more commonplace, disaster recovery (DR) testing (i.e., exercising your company’s disaster recovery plan or strategy) has become more complex. It can be argued that the need for a documented, comprehensive, actionable and accurate technology disaster recovery plan is more important now than ever before.

In the past, when systems, hardware and applications were supported primarily by in-house staff, IT management could point a finger and touch the engineers responsible for their critical systems and applications. Now, IT management must talk with a third-party account executive in order to set up a conversation with their support team. A trouble ticket request is then generated, which is responded to in the order in which it was received.

On its own, this process may seem tedious but certainly not onerous. But when we extrapolate this process flow across multiple platforms, applications, locations and vendors and the following challenges facing IT managers are revealed:

- Multiple assets, managed by multiple parties responsible for your critical data;
- The impact on disaster recovery testing and planning;
- The need to plan and test smarter, not necessarily longer.

Companies hire IT services partners to deliver vendor support for a number of reasons: cost savings, additional expertise, economies of scale and time and additional headcount with collective experience in particular architectures, applications and technology. Companies of all sizes and shapes now need to take advantage of that support and manage it effectively to support their organizations’ DR testing program. Round-the-clock testing is now much more palatable as long as vendor resources are scheduled accordingly. There is no longer a need for company employees to spend their weekends and holidays performing DR exercises, instead vendors and partners can perform those tasks. However, this is an area where vendor relationships - and capabilities - are widely underused and misunderstood.

DR exercise management and pre-test preparation are the keys to utilizing this model to your organization’s advantage. This paper will discuss what pitfalls to avoid and how to update your DR plans so that you are testing the plan and not planning the test. This includes:

- SLA and contract review to understand level of vendor support;
- Validation procedures to insure smooth hand-offs between staff;
- Identifying application owners to manage the end-to-end success within each application;
- Test management to help set goals and objectives, track issues and manage the entire process.
Start with an SLA and contract review

As accommodating as providers tend to be, when it comes to crisis situations it is best to have accurate contract language in place to support every requirement. All vendor contracts should be reviewed to understand what level of support is covered, both at time of test and in the event of a disaster declaration. Most contracts may mention technical support at time of incident, but frequently leave out support at time of test. Your contract should spell out the type and location (remote, onshore or offshore) of technical expertise you can expect when you need it most - during an emergency. Just as important, the contract should cover the same parameters when you test or exercise your DR solution.

The contract review needs to be thorough so that there are no questions or assumptions that are left to chance. Consider the following questions:

- What level of support am I contracted for? Will the same resources that provide daily support to my systems and applications be available at time of incident?
- Is Production support impacted or resources constrained during a DR exercise?
- How many disaster recovery tests per year are covered in my contract?
- How many hours of test support are covered in my services contract?
- Exercise preparation typically includes a substantial amount of pre-work; will support be available to take part in these pre-test planning sessions?
- Similarly, the post-test process usually provides valuable remediation steps to improve the program; will support be provided during these test wrap-up activities?

If you are working with an IT services partner on application development, daily IT operations, or both, you owe it to your organization to understand the level of support contracted for during testing and actual disaster recovery events. Many contracts have vague or grey areas within their documents, especially with regards to DR support, outages, and documentation. Some organizations view their DR restoration procedures as proprietary information. This approach is not a problem, if the vendor can still provide proof that these procedures exist and that the solution they support meets your business requirements.

Partnering with global IT services players is becoming common practice, whether offshore, onshore or even semi-sourcing as with cloud computing and SaaS or IaaS. The more moving parts required to support your organization’s IT environment, the greater the need to strictly manage your DR roles and responsibilities.

One way to help clear the clutter of all these moving parts is to focus an organization’s DR plans around applications; as opposed to platforms. This solves a number of issues caused by multivendor and partner support. These DR plans are designed to pull together servers, data feeds, storage, and gateways, network connectivity and legacy databases— as well as the vendors that support them. Regardless of location, ownership, or vendor support, this plan will identify and list all hardware and software components required to support the said application. The application owner can act at the DR manager to pull all the required staffing resources together at time of test or disaster. An
organization’s DR manager can then administer all application plans as part of their overall DR program, which all leads to more efficient DR exercising and testing.

Once application disaster recovery plans have been developed and exercised, organizations with mature DR programs take their documentation to the next level. More and more organizations are moving to align their DR programs, documentation and recovery solutions with the business processes that they support. This is happening not only at the business unit or department level, but across departments so that an entire critical business process is captured. For example, consider the process required to complete a sale. This would include business unit tasks from marketing, contracting, finance, and of course sales and/or operations.

As these business process DR plans align their solutions and strategies into recovery tiers that support the end user requirements, organizations gain a new sense of comfort because they prove that they can truly operate their business on their DR platforms.

This process is complex to build and needs to be developed in an iterative approach. Comprehensive business and application dependency mapping, business process prioritizations, and associated risks and impacts are some of the required prerequisites, as are business continuity plans that instruct the end user population on the processes and procedures required to utilize the DR solution.

The value of exercising the solution

DR exercise testing is geared to evaluate awareness, validate solutions and procedure documentation, demonstrate fail-over and recovery capabilities and train personnel in expected roles and duties. Today, these duties are performed by multiple vendors, in multiple countries, alongside in-house staff and end users. This adds not only to the complexity of managing a DR program, but to the criticality of implementing it properly. A poorly managed DR program often leads to poor execution at time of need. Poorly executed DR solutions can lead to financial and customer service impacts for organizations that can affect them dramatically. It is acceptable to point fingers following an unsatisfactory DR test or exercise; this becomes a lesson to be learned from. The same is not true following a lengthy delay when returning to normalcy from an actual outage. In this case relationships are severed, contracts cancelled and jobs lost.

Typically, exercises create an opportunity for supporting vendors, and for team members — be they operational, application, or third-party — to execute DR tasks in a simulated environment. DR tests shouldn’t be considered as a pass/fail, but rather exercises to be learned from. All DR exercises provide value to an organization and can be learned from, but it is what happens after the test that shows whether an organization’s DR solution will work or not. Many organizations fail to learn from their DR testing mistakes and thus fail to improve their overall DR programs. As exercises build upon one another, the DR testing program takes shape and provides real value to an organization. It is the responsibility of the DR manager to work with third-party providers to ensure that they embrace this test exercise process the same way they support a system upgrade or an application rollout. It needs to be an expected part of the provider’s contract responsibilities.
DR test methodology roles and documentation, in coordination with an organization’s overall BC/DR program, should include:

- Assumptions, purpose and objectives.
- Overall exercise program objectives that are supported by individual DR test goals.
- Test program elements and design criteria.
- Recovery team roles and members.
- Measurement criteria — test results, remediation schedule, etc.
- Types of testing: table top, functional-sandbox, or alternate site.
- Test frequency and timeline.
- Definitions and templates for individual test plans and guides.

The above mentioned DR exercise program components need to be expanded to support today’s globally virtual organizations. Consider the following:

- Who is responsible for development of restore and/or failover procedures for critical systems and applications?
  - What format will these procedures be delivered in?
  - Will the vendor adhere to the organizational format the company provides?
  - Will these procedures be validated prior to testing?
  - How is the maintenance of procedures accounted for?
  - How are procedure changes incorporated into existing SDLC and change management process?
  - How is it covered in the contract? Is a one-time fee baked in?

- Who is responsible for obtaining copies of binaries and license keys?
  - Who maintains the copies?
  - How is information maintained?

- At time of test, will vendor provide round-the-clock support?

Most DR testing is done in blocks of twenty-four hours. This is where the vendor relationship should really provide value. Instead of in-house company resources burning the midnight oil and giving up weekends to support a DR exercise, the vendor can be asked to provide multiple resources to account for these second and third-shift requirements. Offshore resources are even more convenient due to time zone shifts. One caveat: It is important to obtain a roster of all vendor resources that will support your exercise and the eight-hour shift which they will support. These resources should also be part of pre- and post-test processes. Also ensure that your DR environment (network, core infrastructure, data bases and applications) will support remote access from these support vendors.
Continuous testing and learning

Organizations need to use the post-test process not only to update recovery procedures and hardware requirements, but also to update service contracts based on shortcomings identified during testing.

The DR exercise post-test process is key to the ongoing recoverability of an organization. The issues, concerns, mistakes, upgrades, edits and changes that were identified as part of the DR testing process need to be incorporated into a detailed remediation plan. This remediation plan needs to be incorporated into a freestanding organizational project so these items can be addressed and rectified, progress tracked and accountability assigned — all prior to the next DR test event. Organizations often fall short during this post-test process and as they fail to remediate they find themselves doomed to replicate many of the same issues, errors and mistakes during their next DR test event.

As remediation plans are assigned, and vendors and suppliers are provided with their tasks, tracking and managing this process becomes an important responsibility. Organizations are relying on these remediation plans to lead the effort to update hardware, improve code, procedures and processes. Ultimately this improves their DR capabilities. This process must be managed in order to keep on top of activities to ensure these steps are completed. To successfully manage each post-test initiative, executive reporting should be provided regarding the status of the remediation, and vendors should be held accountable for their role, tasks and issues, as laid out in the remediation plan. IT vendors and partners need to provide support, to improve your DR program - during this relative downtime - with the same level of support they would provide at time of emergency. As stated earlier, if these issues are not resolved, they tend to be repeated at the next test, or worst case, are repeated during an actual emergency.
IMPLEMENTING A BCMS AND GETTING CERTIFIED:
An analysis across geographies

By Dhiraj Lal
**ABSTRACT:** This paper focuses on similarities and differences in the effective implementation of business continuity management across diverse cultures, particularly in emerging/developing markets, such as the Middle East and Africa. The paper argues that any BCM implementer or consultant can increase his or her effectiveness by understanding the organization’s culture and the geography in which it operates and should accordingly tailor-make the BCM implementation approach, for maximum effectiveness.

**Author**

**DHIRAJ LAL**

Dhiraj Lal is executive director and principal consultant of Continuity and Resilience (CORE). He is Asia’s first BSI appointed Technical Expert for BS25999, is a BS25999 assessor and has implemented or assessed BCM in the US, Qatar, Saudi, Bahrain, Abu Dhabi, Dubai, Mauritius and India. He is a BCI approved Instructor and in the past has also instructed for the Disaster Recovery Institute in Asia. Mr. Lal is a post graduate in Management and holds a Bachelors degree in Chemical Engineering.
Introduction

This paper focuses on similarities and differences in the effective implementation of business continuity management (BCM) across diverse cultures, particularly in emerging/developing markets, such as the Middle East and Africa.

As a BSI-approved BS25999 Technical Expert and Assessor, I have personally been involved in the BCM Stage 1 and Stage 2 Assessment of various organizations for BCM certification (so far BS25999, expected also for the ISO22301 also). Additionally, as a BCM consultant, I have been involved in over 20 business continuity management system (BCMS) implementations, including two done largely in Arabic.

This analysis takes into account my experiences with BCM implementation and certification for organizations based in the Kingdom of Saudi Arabia, Qatar, Nigeria, UAE and Bahrain. Organization names will be kept confidential, but the discussion will revolve around their common characteristics and patterns.

The paper argues that any BCM implementer or consultant can increase his or her effectiveness by understanding the organization’s culture and the geography in which it operates and should accordingly tailor-make the BCM implementation approach, for maximum effectiveness.

The importance of organizational culture

Whilst working in the Middle East and Africa Region I observed that there are particular styles and ways of doing things that facilitate effective BCM implementation within certain organizations and geographies. Conversely, if those approaches are not followed, then the implementation is less effective. It would therefore be very useful for BCM professionals to be able to understand what works and what does not work, while looking to implement BCM within the Middle East and Africa.

As one tries to unravel this puzzle, the key element that appears is organizational culture. Interestingly, organizational culture is not a phrase that exists in either the ISO22301 or the BS25999 business continuity management standards. Nevertheless, the organizational style and approach has a lot to contribute towards the process of BCM implementation and embedding.

Yet, while we speak about Africa and the Middle East in one breath, is this really useful at all? Can one generalise across these two large geographies? As persons living in or visiting those areas, we certainly gain views and observations about the ‘regional’ culture, but it soon becomes clear that each country in the region has its own unique culture.

In order to understand the differences more clearly in order to inform regional BCM implementations, I located a research study (1) which directly compared on a quantitative basis the shared values (2) of a multinational corporation across its Middle East and Sub-Saharan subsidiaries. The study superimposed 24 shared values on the Competing Values Framework (CVF) (3), a methodology and tool used to measure organizational effectiveness. The research found that the 24
shared values do not differ across geographies, except for broad-mindedness, development and orderliness.

For the Middle East, the most important value was broad-mindedness, followed by humour, adaptability and initiative. Creativity, forgiveness and diligence were also important values. The least preferred value was autonomy. Aggressiveness and formality were also values that were frowned upon.

Further, the core dimensions of the CVF depict four organizational forms: clan, adhocracy, market and hierarchy. For the Middle East the ranking of these in order of priority was:

1. **Clan** – emphasises morale and group cohesion; places an importance on human relations with flexible operations and procedures. It is the direct opposite of market culture.
2. **Market** – emphasises efficiency and productivity; result-oriented, assertive and competitive.
3. **Adhocracy** – emphasises transformation and growth; encourages people to ‘stick out their necks’ and take risks. It is the direct opposite of hierarchy.
4. **Hierarchy** – based on clear task-setting and enforcement of strict rules. Emphasis on formally, order and respect.

It is to be noted that the most sought after of the 24 values were within clan, whilst the least were within adhocracy.

The above means that, in general, a BCM implementation style that emphasises relationships and consensus may be more effective in the Middle East; and a style which is aggressive and pushy may be much less effective.

**Lessons from case studies**

Do real-life case studies validate the above conclusions? In order to verify this, I looked at the observed realities on the ground for past implementations and success stories and separated the observed BCM implementations into two categories of customers:

- Older ‘matured BCM implementations’
- Newer ‘must get certified soon’ implementations.

Within these two groups clear differences in approach could be seen.

In older ‘matured BCM implementations’, the BCM consultants involved in the implementation were typically those with a strong brand name; and often using a standardised ‘cookie-cutter’ approach. In many cases these implementations have not been very successful. Organizations have typically used multiple consultants, and the BCMS has gone through various versions.

Most newer implementing organizations had adopted a strategy of hiring consultants to help them implement BCM. For more recent implementations, the consultants were typically highly specialised and with proven competencies, typically with a local presence, normally referred to them by a known associate in the field.
In the most recent and accelerated implementations, the driver for implementing BCM has typically come from senior management, typically the CEO/Board/C level. A senior manager has typically been given the BCM responsibility, and the consultant has been tasked not only to implement BCM, but retained until the company receives its BCM certification. There has been a large emphasis on BCM training, typically as an inhouse effort, inter-woven as a just-in-time approach with the BCM implementation. Given the fact that such countries would typically have only scarce BCM resources in-country, one would expect a high level of utilisation of BCM eLearning – but this was not the case. Perhaps one constraint being a not-so-good communications/technology infrastructure in some places, as well as local language issues with available eLearning products.

BCM involvement in most cases is mandated right from the top – and in most of these cultures people down the line have taken to that mandate quite enthusiastically. So there has been a lot of ‘buzz,’ visibility and excitement regarding the BCM implementation. Senior Management oversight and overt keenness for the project has helped to keep things on track. The size of the BCM team has typically been small, with BCM in many cases being not even a full-time function – just a hat being worn on a part time basis.

In the more matured BCM implementations, the size of the BCM team was typically three - four persons. These organizations typically had a highly respected senior manager with direct responsibility for the full-time BCM team, in most cases a local who had been with the organization for quite a few years. The BCM core team normally has deep domain knowledge and a high degree of maturity in BCM. The department coordinators have also been exposed to BCM for over three-five years and are typically quite competent in their own right. The process had matured to an extent that the CEO no longer needs to drive BCM: this by now has become a concept that is widely percolated across the organization. Therefore, even the emphasis on awareness training had decreased somewhat, and BCM had now become a normal business process. Yet, in many of these cases BCM was “just another Management System Implementation” - and therefore implemented without much fanfare, often as part of the overall risk management framework.

In most of the BCM implementations, both recent and matured, the organizations have liberally invested in in-country backup infrastructure - possibly driven by the fact that these being relatively nascent BCM geographies, there really were no option to lease or partner: instead these organizations had to build. So the quality of the recovery infrastructure was quite high, overall, as was the emphasis on testing and exercising. Almost all these organizations had invested heavily in training, both for the core BCM team, as well as for the department coordinators.

The smarter organizations with lean teams and large BCM scope have started to implement BCM tools – but those are exceptions. As a general rule these organizations had not looked actively at BCM tools. Instead, the approach was more to manage through people and manual processes rather than BCM tools.
Summary

In summary, analysis of BCM implementation and certification across newly-emerging BCM geographies reveals some interesting patterns in the approaches adopted by the organizations to implement BCM and eventually get certified. A good understanding of these successful approaches can be helpful in establishing principles of effective BCM implementation across such geographies and cultures.

Note

The original version of this paper was presented at the BCM 2012 World Conference and Exhibition.

References


(2) McDonald & Gandz (1992) *Getting value from shared values*. Organizational Dynamics

(3) Quinn, R.E and Rorbaugh, J (1983) *A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis*. Management Science
RESEARCH ROUNDUP
SUMMARIES OF RECENT COMMERCIAL AND ACADEMIC BUSINESS CONTINUITY AND RESILIENCY RESEARCH

Contents

- Disaster recovery trends and metrics
- Internet outages in the US doubled during Hurricane Sandy
- Social media is often a reputation management ‘blind spot’
- There's a hole in many business continuity strategies: cloud application backup
- The adoption of BCM standards and ISO 22301
- Supply Chain Resilience 2012
- Unscheduled server/workstation downtime in the United States
- Supply chain focus can make the difference between organizational growth and failure post-crisis
DISASTER RECOVERY TRENDS AND METRICS

FalconStor Software, Inc. has published the results of its ‘Disaster Recovery Trends and Metrics’ survey which was conducted in partnership with IDG Research Services. Featuring responses from 189 IT managers and executives, the poll found that 42 percent of respondents were still not adequately armed with modern disaster recovery solutions, even though they experienced at least one instance of data loss in the past year.

Many of those surveyed continue to rely on manual processes and tape backup systems; however, most respondents anticipate an evolutionary move toward highly available, automated systems with data replication within the next 18 months.

The survey also found that tape backup was the most pervasive data backup solution, with 23 percent of large enterprises, 48 percent of medium enterprises and 27 percent of small businesses relying on this technology.

Additional survey findings included:

- Sixty-five percent of respondents reported using manual disaster recovery processes; however, 83 percent reported that they believe automated disaster recovery and data replication technologies will be more widely used in the next 18 months.
- Seventy-two percent of overall IT leaders stated that their disaster recovery plans are only tested an average of once a year, with 82 percent of large enterprises completing disaster recovery testing one or more times yearly as compared to 75 percent of medium enterprises and 63 percent of small businesses.
- Forty-two percent of respondents said their organizations experience at least one data outage per year, with an average of 34 instances across enterprises of all sizes; of these companies, the majority of respondents stated that downtime in excess of four hours for any outage is unacceptable.
- Fifty-three percent of organizations responded that an outage of more than four hours is unacceptable, with the most common consequence being loss of productivity (as reported by 67 percent), followed by 27 percent reporting harm to reputation, financial loss and loss of irreplaceable data.

The online poll conducted by IDG Research collected information from 189 IT leaders across all market segments that were using or planning to use disaster recovery and data protection technologies. Thirty-two percent of these individuals worked at firms with more than 5,000 employees; 23 percent of these individuals had between 1,001 and 5,000 employees; 37 percent of these individuals had between 101 and 1,000 employees; and eight percent had between 50 and 100 employees at the time of the survey.
INTERNET OUTAGES IN THE US DOUBLED DURING HURRICANE SANDY

USC scientists who track Internet outages throughout the world noted a spike in outages due to Hurricane Sandy, with almost twice as much of the Internet down in the US as usual.

Previous research by this team has shown that on any given day, about 0.3 percent of the Internet is down for one reason or another. Just before Hurricane Sandy hit the East Coast, that number was around 0.2 percent in the US – but once the storm made landfall, it jumped to 0.43 percent and took about four days to return to normal.

The above findings are detailed in a new report by scientists at the Information Sciences Institute (ISI) at the USC Viterbi School of Engineering.

"On a national scale, the amount of outage is small, showing how robust the Internet is. However, this significant increase in outages shows the large impact Sandy had on our national infrastructure," said John Heidemann, who led the team that tracked and analysed the data. Heidemann is a research professor of computer science and project leader in the Computer Networks Division of ISI.

Heidemann worked with graduate student Lin Quan and research staff member Yuri Pradkin, both also from ISI, sending tiny packets of data known as ‘pings’ to networks and waiting for ‘echoes,’ or responses. Though some networks—those with a firewall—will not respond to pings, this method has been shown to provide a statistically reasonable picture of when parts of the Internet are active or down.

The team was also able to pinpoint where the outages were occurring, and noted a spike in outages in New Jersey and New York after Sandy made landfall.

The research was funded by the US Department of Homeland Security Science and Technology Directorate.

SOCIAL MEDIA IS OFTEN A REPUTATION MANAGEMENT ‘BLIND SPOT’

Zeno Group has published findings from the Zeno Digital Readiness Survey, which found that many organizations are failing to consider their social media reputation. In fact, more than one-third of executives (36 percent) say that the CEO of their company does not care or cares little about the company’s reputation in social media. In addition, while most organizations say they would take some action to respond to an online crisis, at least 10 percent report their organizations would not take any action at all to engage with audiences online to address a damaging article or social media post.

The online survey polled 300 US corporate executives, spanning a range of industries and titles of VP or higher, including C-suite executives, such as CEOs, presidents and chairmen. Notably, over half of
respondents described their firms as primarily business-to-business (B2B) companies, and all companies had annual revenues of at least $1 billion.

From a sector view, the Zeno Digital Readiness Survey reveals a stark difference between B2C (business-to-consumer) and B2B companies in not only executive attitudes toward social media, but also in their ability to respond to an online challenge.

Specifically, the Zeno Digital Readiness Survey finds that:

- **B2B companies lag their B2C counterparts when considering social media reputation.** B2C-focused executives say their company's CEO frequently considers social media reputation in their decision-making, with 70 percent indicating it's 'always' or 'sometimes' a factor, compared to 57 percent of B2B executives. This leaves a significant number of B2B executives (43 percent) who indicate that the CEO largely ignores their company's online reputation, compared to only 30 percent from the B2C sector.

- **B2C companies are prepared to respond more quickly to online audiences in a crisis.** 63 percent of B2C executives believe their firms could respond to a negative online post within 24 hours compared to only 45 percent of B2B executives.

- **B2B companies are less likely to engage online in a crisis.** B2B executives are twice as likely to say that their firm would not engage an audience online at all to defend their reputation (13 percent, compared to 6 percent of B2C executives).

The overall findings suggest that social media is a corporate reputation ‘blind spot,’ especially for B2B companies – a concerning notion considering that social media now accounts for almost a quarter of people's time spent online. As a result, companies that continue to ignore the online community or dismiss its influence are putting their reputations at risk.

Attitudes toward social media reputation also appear to differ by company size. Executives in larger firms (with more than 10,000 employees) are more likely to say their CEO always or sometimes considers their company’s social media reputation, as compared to those at companies with less than 10,000 employees (71 percent versus 55 percent, respectively). Among smaller firms, the tendency to ignore social media reputation is even more pronounced; 45 percent indicate it is rarely or never considered in decision-making, compared to 29 percent of larger firms.

Similarly, when looking at company size by revenue, larger firms are also more likely to respond quickly to a damaging issue online, with a majority of the largest firms (with revenue of $10 billion or more) saying they could react within 24 hours (63 percent), in contrast to 42 percent of smaller firms (less than $5 billion in revenue).
THERE’S A HOLE IN MANY BUSINESS CONTINUITY STRATEGIES: CLOUD APPLICATION BACKUP

Asigra has released information from a recent survey, highlighting the growth in SaaS and cloud-based business application services and the need for more comprehensive data protection strategies to ensure business continuity and compliance.

The enterprise survey, commissioned by Asigra and performed by the customer metrics and research organization, TechValidate, found that enterprises have endorsed SaaS and the cloud as a viable business application platform, with 55 percent of the organizations surveyed using Salesforce.com and 74 percent expecting the use of other SaaS/cloud-based applications to increase. Of the cloud-based CRM applications in use, Salesforce.com showed the highest level of deployment at 23 percent followed by Microsoft Dynamics at 12 percent, Oracle at 12 percent, SAP at 8 percent and Sugar CRM at 4 percent. Of those same respondents, however, only 22 percent indicated that SaaS/cloud-based application data is incorporated into their corporate backup infrastructure.

Of the backup and recovery solutions that organizations have in place, most rely on a mix of solutions. The TechValidate survey showed that 66 percent of those surveyed have some form of physical device backup solution. 41 percent use a virtual machine backup solution while 38 percent use tape backup, 24 percent have a cloud/online backup solution and 7 percent rely on USB hard drives for backup. When asked what attributes they consider most important in a backup solution when protecting cloud-based application data, 68 percent said a comprehensive backup solution that protects both cloud and on-premise applications is desired, 52 percent said the solution must be fast and highly secure while 10 percent indicated a stand-alone cloud application backup solution would meet their needs.

Concerns over the storage of data in the cloud were not surprising. Of those surveyed, 21 percent cited data security as the biggest concern while the location of where the data was stored came in at 7 percent. Backup related costs, user-related data loss and service provider stability all ranked at 3 percent. 59 percent said that all of these were concerns with respect to storing data in the cloud.

To view the TechValidate visit http://www.slideshare.net/Asigra/asigra-cloudtocloud-survey-results-15282436

THE ADOPTION OF BCM STANDARDS AND ISO 22301

The Business Continuity Institute has published part two of a survey into business continuity standards.

The first part was published earlier in the year and considered awareness levels of the ISO 22301 business continuity standard. The second part of the study looked at who is involved in the decision making process to adopt ISO 22301; whether there is a requirement to develop a business case; and what the perceived transition issues are.
The field work for the survey started on April 24th and closed on May 17th 2012 and attracted 613 responses. Respondents were drawn from more than sixty countries and 15 industry sectors.

The key findings were:

- Few BCM professionals see the need to go beyond the business continuity discipline to get a decision to align with the ISO 22301 standard, but with certification almost 75 percent will need to convince someone outside the discipline.
- 48 percent of respondents stated that they need a business case to adopt ISO 22301. However, the decision process and requirement for a business case is made easier if the organization holds an existing certification.
- When asked why their organization would not go down the ISO22301 route, respondents summarised the reason in terms of ‘lack of drivers’. Without a customer or regulatory requirement, they saw no reason to do so. Others stated they were happy with their existing approach and that the ISO did not offer anything new.

Read the full survey report after registration at http://www.thebci.org/index.php?option=com_content&view=article&id=313&Itemid=267

**SUPPLY CHAIN RESILIENCE 2012**

The Business Continuity Institute has published a new report into supply chain resilience which finds that 73 percent of organizations recorded at least one supply chain disruption in 2011.

The report summarises the key outcomes of the BCI’s 4th Annual Supply Chain Resilience Survey. 532 people from across 68 countries and 14 different industry sectors responded to the survey, which was supported by the Chartered Institute of Purchasing & Supply, Zurich Insurance Group and DHL Supply Chain.

The survey concludes that effectively managing supply chain continuity is critical not just because of the immediate costs of disruption, but also the longer term consequences to stakeholder confidence and reputation that may arise following a supply chain failure.

Further findings included:

- The leading cause of supply chain disruption is unplanned IT or telecom outages with 52 percent of organizations surveyed experiencing some or high impact disruption as a result, followed in second place by adverse weather, experienced by 48 percent of respondents;
- Currency volatility rises to fourth place in this survey of disruption. While not traditionally seen as a business continuity area, it shows that business continuity thinking can be more widely applied;
- Disruption is also becoming more consequential – financial costs are higher than in 2011 with one in five companies registering a single incident loss of more than €1 million;
- The UK leads the USA in considering supply chain disruption within continuity programmes with 75 percent doing so in the UK compared to only 44 percent of US-based respondents.
UNSCHEDULED SERVER/WORKSTATION DOWNTIME IN THE UNITED STATES

Paragon Software Group recently conducted a survey among 377 IT professionals to look at the prevalence and causes of unscheduled server/workstation downtime.

The survey found that over half (51.9 percent) of the businesses surveyed have experienced unscheduled downtime once or twice during the last 12 months. Further, 17.6 percent of those surveyed cite that unplanned downtime occurred more than twice during the year.

Respondents stated the following reasons for the cause of the downtime:

- Hardware failure: 39.4 percent
- Power outages: 22.1 percent
- Operating system failure: 12.1 percent
- Human error: 13.2 percent
- Natural disaster: 5.1 percent.

Other downtime causes cited by respondents included malicious cyber attacks, software errors and fire.

31.7 percent of survey respondents stated that their organization did not have a business continuity or disaster recovery plan.

SUPPLY CHAIN FOCUS CAN MAKE THE DIFFERENCE BETWEEN ORGANIZATIONAL GROWTH AND FAILURE POST-CRISIS

When examining the dynamic between corporate reputation and financial performance, it is important to study the effects of large-scale crises, whether manmade or driven by external forces. Events such as the Japan tsunami and earthquake as well as various accounting scandals, have caused many organizations to lose value, according to the Aon-sponsored Reputation Review 2012 report recently issued by Oxford Metrica, an independent analytics and advisory firm.

Seven of 10 companies measured in the report that were impacted by disasters in 2011 lost more than one-third of their value and two companies lost almost 90 percent.

"While the principles of reputation recovery are made more vivid by crisis, they apply equally to lesser events that can still damage a company's reputation," said Randy Nornes, executive vice president with Aon Risk Solutions. "Last year's research revealed that 80 percent of firms will lose 20 percent of their value once every five years due to reputational issues. Any company – no matter its size – can mitigate the risks of an event by taking a positive and thoughtful approach to crisis
management. Supply chain risk is often the catalyst for crises, so this can be a great place to start the process."

"From business interruption to customer service and quality control, organizations have quickly learned to appreciate the volatility that can stem from a poorly managed supply chain," added Dr. Deborah Pretty, principal of Oxford Metrica.

A coherent reputation strategy can be the difference between recovery and failure for many companies. It can minimize the likelihood of a critical event turning into a reputation crisis and will maximize the probability of recovery. Those that have a firm grip on their brand and are actively monitoring it can more easily weather a crisis. In fact, the research shows that companies that successfully navigate a crisis can actually build additional value.

Best practices that companies should perform to ensure an effective reputation strategy is in place include:

- Evaluate reputation equity to benchmark the effectiveness of your current reputation strategy;
- Analyse the drivers of reputation risks to allocate your financial resources more effectively;
- Develop a reputation recovery strategy to generate the best chance of recovery in the event of a crisis;
- Monitor reputation equity to provide senior management with crucial and timely feedback, enabling confident decision-making and rapid responses to emerging risks.

Copyright

The Business Continuity and Resiliency Journal is Copyright 2012 Continuity Central, all rights reserved.

ISSN

ISSN 1752-4539

Contacts

Continuity Central
1964 Gallows Road, Suite # 210
Vienna, Virginia 22182 USA
PH: 1-703-891-6780
Fax: 1-703 356-7096

Editor

David Honour
editor@businesscontinuityjournal.com

Subscriptions

subs@businesscontinuityjournal.com

Website

www.businesscontinuityjournal.com